SETRAC COLLEGE OF OFFSHORE TRAINING

SHIP SECURITY OFFICER

ISSUE DATE – Oct 2017		
DATE	REVISION	REVISED BY
01 Jan 2016	Rev 01	Training Coordinator
01 Jan 2020	Rev 02	Training Coordinator
01 Jan 2023	Rev 03	Training Coordinator
1 Jan 2024	Rev 04	Training Coordinator

INDEX

Chapter 1

Introduction

Course Objective

Those who successfully complete the course should be able to demonstrate sufficient knowledge to undertake the duties assigned under the VSP. This knowledge shall include, but is not limited to:

1. knowledge of current security threats and patterns;
2. recognition and detection of weapons, dangerous substances and devices;
3. recognition, on a non-discriminatory basis, of characteristics and behavioral patterns of persons who are likely to threaten security;
4. techniques used to circumvent security measures;
5. crowd management and control techniques;
6. security related communications;
7. knowledge of emergency procedures and contingency plans;
8. operation of security equipment and systems;
9. testing, calibration and at-sea maintenance of security equipment and systems;
10. inspection, control, and monitoring techniques; and
11. methods of physical searches of persons, personal effects, baggage, cargo, and vessel stores.

Course overview

This model course is intended to provide the knowledge required for vessel personnel who are assigned specific security duties in connection with a Vessel Security Plan (VSP) to perform their duties in accordance with the requirements of the Maritime Transportation Security Act of 2002 and/or Chapter XI-2 of SOLAS 74 as amended and/or the IMO ISPS Code and/or U.S. Coast Guard regulations contained in 33 CFR Chapter 1 Subchapter H.

Competences to be achieved

1. Every seafarer who is designated to perform security duties, including anti-piracy and anti-armed-robbery-related activities, shall be required to demonstrate competence to undertake the tasks, duties and responsibilities listed in column 1 of table A-VI/6-2.

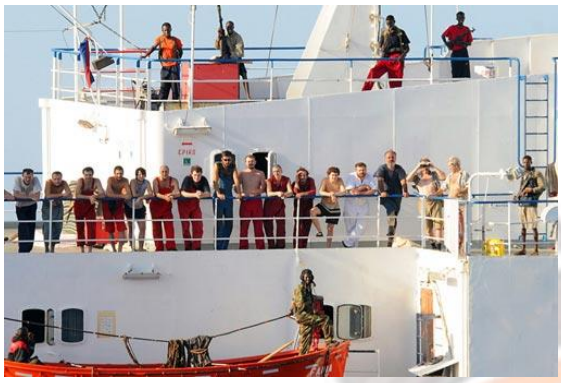
2. The level of knowledge of the subjects in column 2 of table A-VI/6-2 shall be sufficient to enable every candidate to perform on board designated security duties, including anti-piracy and anti-armed-robbery-related activities.

3. Every candidate for certification shall be required to provide evidence of having achieved the required standard of competence through:

> 3.1 demonstration of competence to undertake the tasks, duties and responsibilities listed in column 1 of table A-VI/6-2, in accordance with the methods for demonstrating competence and the criteria for evaluating competence tabulated in columns 3 and 4 of that table; and

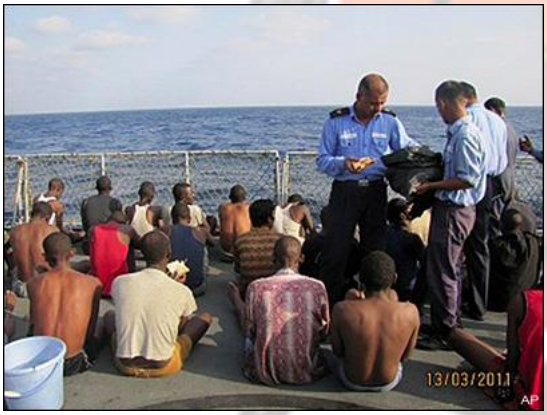
3.2 examination or continuous assessment as part of an approved training programme covering the material set out in column 2 of table A-VI/6-2.

Current security threats and patterns



Piracy and armed attacks continue to occur on an all too frequent basis. Attacks occur mostly in portareas, whereas piracy, by definition, usually involves ships at sea. In fact, the United Nations Convention on the Law of the Sea, Article 101, defines piracy as any of the following acts: illegal acts of violence or detention or any act of depredation committed for private ends by the crew or the passengers of a private vessel or private aircraft and directed on the high seas against another vessel or aircraft or against persons or property on board such vessel or aircraft. It also includes such acts against a vessel, aircraft, person or property in a place outside of the jurisdiction of any State.

Terrorism usually involves violence, or the threat of violence, by extremist groups seeking to gain political objectives by malicious means. A terrorist group may hope to make a statement by using various types of bombs, making bomb threats or hijacking a vessel. Increasingly, terrorists are acting in connection with extremist religious sects that promote suicidal behavior. Contraband smuggling, a criminal activity, may result in large financial loss to the vessel owner whose vessel is being used by the smugglers. Often, drugs are the commodity being smuggled and they may be brought on board in a number of creative ways such as in luggage, stores, on or in a person's body, or in electronic equipment. Weapons are also a frequent item associated with smuggling. Like drugs, weapons, too, find their way on board in various ways, such as in cargo containers.



Cargo theft, an age-old problem, continues to plague the maritime industry and causes financial losses in staggering amounts. Prevention is normally the most effective method of dealing with this security threat.

Security Threat at Sea

The attack, stated to be by Al Qaeda, on the US naval ship USS Cole at Aden in October, 2000, and the subsequent investigation into that incident gave birth to concerns that international terrorists might expand their acts of terrorism from the land to the sea. Terrorist groups of West Asia and the Liberation Tigers of Tamil Eelam (LTTE) had indulged in acts of maritime terrorism even before October, 2000, and the LTTE, through its fleet of ships, ostensibly used for legitimate commercial purposes, had been using the sea for the clandestine transport of arms and ammunition and other material required for its acts of terrorism on the land. However, such uses had limited tactical objectives and did not think in terms of mass casualties or mass damage to be inflicted on the global economy as a whole.

The 9/11 terrorist strikes in the US and the precision and the evil ingenuity with which they were planned and executed created a wave of alarm about the likelihood of similar strikes at coastal and maritime targets. Since 9/11, there is hardly any discussion, governmental or non-governmental, on threats to national security and to international peace and security in which possible threats from maritime terrorism do not figure prominently.Post-9/11, scenario-building exercises have invariably included scenarios involving possible catastrophic acts of maritime terrorism. Four of these possible scenarios are or should be of major concern to national security managers:

First, terrorists hijacking a huge oil or gas tanker and exploding it in mid-sea or in a major port in order to cause huge human, material and environmental damage. There were 67 reported attacks on oil and gas tankers by pirates during 2004. This despite the stepped-up patrolling by the Navies of different countries. What pirates with no ideological motive and with no suicidal fervour can do, ideologically-driven suicide terrorists can do with equal, if not greater, ease. Second, terrorists hijacking an oil or gas tanker or a bulk-carrier and exploding it or scuttling it in maritime choke-points such as the Malacca Strait in order to cause a major disruption of energy supplies and global trade. There were 52 reported attacks on bulk carriers by pirates during 2004. If the pirates can do it despite naval patrolling, so can the terrorists.Third, terrorists smuggling weapon of mass destruction material such as radiological waste or lethal chemicals or even biological weapons in a container and having it exploded through a cellular phone as soon as the vessel carrying the container reaches a major port.Fourth, sea-borne terrorists attacking a nuclear establishment or an oil refinery or off-shore oil platforms.

Vessel Personnel with Specific Security Duties

Although there may not be violence or political issues involved in most cargo theft cases, this matter remains high on the list of security threats and requires solutions discussed in this course. Instructors should convey that cargo theft is only one of the various threats to the security of cargo. Other such security threats should be discussed during this section of the course.Collateral damage occurs when a nearby fire, explosion, or attack results in damage to a vessel or facility. While the damage is sometimes unintended, the costs are nevertheless real. There are measures that may minimize the consequences of this type of damage.

Chapter 2

Maritime Security Policy

Maritime Security

The term maritime security represents the broadest approach to issues and aspects which pertain to the sea and have an important bearing on the country's security.. This volume would go a long way in generating fuller understanding of the different aspects of the maritime dimensions of India's security.

As the seas of peninsular India and the Indian Ocean become more important than even before to the security of the country, it is imperative to examine the maritime dimensions of Indian security in a comprehensive manner. India's Maritime security provides, for the first time, a holistic assessment of the economic, political, and military aspects of India's maritime security.

The term maritime security is defined as comprising those issues which pertain to the sea and have a critical bearing on the country's security. These include seaborne trade and commerce in energy resources, the management of living and non-living marine resources, the delimitation of international seaward boundaries, and the deployment and employment of naval and military forces in the Indian Ocean.

Maritime Security Policy

All nations and port authorities can benefit from a coordinated policy for maritime security ctivities that involve cooperation with foreign governments, international and regional organisations, and the private sector.

The oceans are the largest part of the surface of our planet, a continuous domain with few visible traces of nations' 'territorial seas' and 'exclusive economic zones.'The oceans are largely borderless, and in countries with coastlines the many agencies responsible for maritime security have overlapping territories and mandates, which makes coordination and information sharing absolutely necessary in today's security environment.

Different nations' agencies assign security roles in different ways, but the need for information sharing is the same.In India Maritime Security is looked after by Navy and Coast Guard. In the recent years the Police department have also started developing infrastructure and expertise for coastal security. DG Shipping certifies the security of ships and ports.

A large number of US maritime security policy documents explicitly state the need for cooperation with the agencies of other governments and with scores of international, regional and industry organisations, many of which are listed in an appendix to the US State Department's International Outreach and Coordination Strategy for the National Strategy for Maritime Security (NSMS), released in November 2005.

Plans for port security programmes include terms like 'maritime intelligence integration,' 'coordinated response,' and 'standardised procedures.'The previously mentioned document includes this sentence "maritime domain awareness will be achieved by improving our ability to collect, fuse, analyse, display, and disseminate actionable information and intelligence to operational commanders and decision makers.Geospatial interoperability refers to the ability of diverse systems to transparently exchange

diverse kinds of geospatial information and services and to support the query/response mechanisms of geospatial Web services.

Such communication depends on transmitting or exchanging through a common system of interfaces and encodings. Standardisation means 'agreeing on a common system,' so standardisation on interface and encoding specifications is a maritime security, and port security, requirement.Criminals and individual terrorists who belong to international networks are more likely to be noticed by civil sector agencies than by defense agencies.

Because maritime domain awareness requires that both defense and civil sector agencies be able to "collect, fuse, analyse, display, and disseminate actionable information and intelligence," it is important that the same geospatial standards are being agreed upon by both types of agencies.

Regulations

The International Maritime Organization (IMO) has adopted a number of resolutions and conventions to this end. For example, Resolution A.545(13)--Measures To Prevent Acts Of Piracy And Armed Robbery Against Ships was signed in 1983. In 1985 came IMOResolution A.584 (14)--Measures To Prevent Unlawful Acts Which Threaten Safety Of Ships AndSecurity Of Passengers (this was later reviewed in November of 2001 with IMO Resolution A.924(22)).

Then in 1986 the IMO approved MSC/Circ.443--Measures To Prevent Unlawful Acts Against Passengers And Crew On Board Ships. In 1988, the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA) treaties aimed at ensuring that appropriate judicial action is taken against persons committing unlawful acts against ships. Unlawful acts would include the seizure of vessels by force, acts of violence against persons on board vessels, and placing devices on board a vessel which are likely to destroy or damage it. The convention obliges contracting governments either to extradite or prosecute alleged offenders. The SUA came into effect on March 1, 1992.

Following the tragic events of September 11, 2001 the twenty-second session of the IMO, in November of 2001, unanimously agreed to incorporate security regulations. They approved the development of new measures relating to the security of vessels and of port facilities for adoption by a Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974 in December of 2002 (the Diplomatic Conference). This timetable of little more than a year represents a landmark achievement for IMO. It provides a clear indication of the gravity of the situation as well as the intention to protect world shipping against security incidents and threats.

The meeting of the Diplomatic Conference in December of 2002 resulted in amendments to SOLAS 74. These amendments enter into force on July 1, 2004. A brief summary of these amendments should be carried out with mention of changes to Chapter V but with emphasis on the changes to Chapter XI, Regulations 3 and 5 and the new Chapter XI-2 Regulations 1-13 and the ISPS Code.

Definitions

2.1 For the purpose of this part, unless expressly provided otherwise:

.1 *Convention* means the International Convention for the Safety of Life at Sea, 1974 as amended.

.2 *Regulation* means a regulation of the Convention.

.3 *Chapter* means a chapter of the Convention.

.4 *Ship security plan* means a plan developed to ensure the application of measures on board the ship designed to protect persons on board, cargo**,** cargo transport units, ship.s stores or the ship from the risks of a security incident.

.5 *Port facility security plan* means a plan developed to ensure the application of measures designed to protect the port facility and ships, persons**,** cargo, cargo transport units and ship.s stores within the port facility from the risks of a security incident.

.6 *Ship security officer* means the person on board the ship**,** accountable to the master**,** designated by the Company as responsible for the security of the ship, including implementation and maintenance of the ship security plan and for liaison with the company security officer and port facility security officers.

.7 *Company security officer* means the person designated by the Company for ensuring that a ship security assessment is carried out; that a ship security plan is developed, submitted for approval, and thereafter implemented and maintained and for liaison with port facility security officers and the ship security officer.

.8 *Port facility security officer* means the person designated as responsible for the development, implementation, revision and maintenance of the port facility security plan and for liaison with the ship security officers and company security officers.

.9 *Security level 1* means the level for which minimum appropriate protective security measures shall be maintained at all times.

.10 *Security level 2* means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.

.11 *Security level 3* means the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.

2.2 The term .ship., when used in ISPS Code, includes mobile offshore drilling units and high-speed craft as defined in regulation XI-2/1.

2.3 The term .Contracting Government. in connection with any reference to a port facility, when used in sections 14 to 18, includes a reference to the .Designated Authority.

2.4 Terms not otherwise defined in this part shall have the same meaning as the meaning attributed to them in chapters I and XI-2.

Handling sensitive security-related information and communications

Ship communicate internally as well as with external agencies on various matters of ship operation. Some of this information may be sensitive and may jeoperdise the ship safety in case it is leaked to unautorised personnel.It therefore needs to be appreciated that certain information and communications will be considered security sensitive and that the level of sensitivity may change, as do levels of security 1, 2, and 3. Seemingly benign conversations, therefore, may result in disastrous consequences. All personnel will need to appreciate the risk of security leaks through communication by improper methods or to the wrong persons.

Chapter 3

Security Responsibilities

RESPONSIBILITIES OF CONTRACTING GOVERNMENTS

Subject to the provisions of regulation XI-2/3 and XI-2/7, Contracting Governments shall set security levels and provide guidance for protection from security incidents. Higher security levels indicate greater likelihood of occurrence of a security incident. Factors to be considered in setting the appropriate security level include:

.1 the degree that the threat information is credible;
.2 the degree that the threat information is corroborated;
.3 the degree that the threat information is specific or imminent; and
.4 the potential consequences of such a security incident.

Contracting Governments, when they set security level 3, shall issue, as necessary, appropriate instructions and shall provide security related information to the ships and port facilities that may be affected. Contracting Governments may delegate to a recognized security organization certain of their security related duties under chapter XI-2 and this Part of the Code with the exception of:

.1 setting of the applicable security level;
.2 approving a Port Facility Security Assessment and subsequent amendments to an approved assessment;
.3 determining the port facilities which will be required to designate a Port Facility Security Officer;
.4 approving a Port Facility Security Plan and subsequent amendments to an approved plan;
.5 exercising control and compliance measures pursuant to regulation XI-2/9; and
.6 establishing the requirements for a Declaration of Security.

Contracting Governments shall, to the extent they consider appropriate, test the effectiveness of the Ship or the Port Facility Security Plans, or of amendments to such plans, they have approved, or, in the case of ships, of plans which have been approved on their behalf.

Recognized Security Organizations

States may delegate some of their responsibilities to RSO who may then may take on the security-related activities of a contracting government.

OBLIGATIONS OF THE COMPANY

The Company shall ensure that the ship security plan contains a clear statement emphasizing the master.s authority. The Company shall establish in the ship security plan that the master has the overriding authority and responsibility to make decisions with respect to the safety and security of the ship and to request the assistance of the Company or of any Contracting Government as may be necessary.

The Company shall ensure that the company security officer, the master and the ship security officer are given the necessary support to fulfil their duties and responsibilities inaccordance with chapter XI-2 and this Part of the Code.

SHIP SECURITY

A ship is required to act upon the security levels set by Contracting Governments as set out below.

At security level 1, the following activities shall be carried out, through appropriate measures, on all ships, taking into account the guidance given in part B of ISPS Code, in order to identify and take preventive measures against security incidents:

.1 ensuring the performance of all ship security duties;
.2 controlling access to the ship;
.3 controlling the embarkation of persons and their effects;
.4 monitoring restricted areas to ensure that only authorized persons have access;
.5 monitoring of deck areas and areas surrounding the ship;
.6 supervising the handling of cargo and ship.s stores; and
.7 ensuring that security communication is readily available.

At security level 2, the additional protective measures, specified in the ship security plan, shall be implemented for each activity detailed in section 7.2, taking into account the guidance given in part B of ISPS Code.

At security level 3, further specific protective measures, specified in the ship security plan, shall be implemented for each activity detailed in section 7.2, taking into account the guidance given in part B of ISPS Code. Whenever security level 2 or 3 is set by the Administration, the ship shall acknowledge receipt of the instructions on change of the security level.

Prior to entering a port or whilst in a port within the territory of a Contracting Government that has set security level 2 or 3, the ship shall acknowledge receipt of this instruction and shall confirm to the port facility security officer the initiation of the implementation of the appropriate measures and procedures as detailed in the ship security plan, and in the case of security level 3, in instructions issued by the Contracting Government which has set security level 3. The ship shall report any difficulties in implementation. In such cases, the port facility security officer and ship security officer shall liase and co-ordinate the appropriate action than that set for the port it intends to enter or in which it is already located, then the ship shall advise, without delay, the competent authority of the Contracting Government within whose territory the port facility is located and the port facility security officer of the situation. In such cases, the ship security officer shall liaise with the port facility security officer
and co-ordinate appropriate actions, if necessary.

An Administration requiring ships entitled to fly its flag to set security level 2 or 3 in a port of another Contracting Government shall inform that Contracting Government without delay. When Contracting Governments set security levels and ensure the provision of security level information to ships operating in their territorial sea, or having communicated an intention to enter their territorial sea, such ships shall be advised to maintain vigilance and report immediately to their Administration and any nearby coastal States any information that comes to
their attention that might affect maritime security in the area.
When advising such ships of the applicable security level, a Contracting Government shall, taking into account the guidance given in the part B of ISPS Code, also advise those ships of any security measure

that they should take and, if appropriate, of measures that have been taken by the Contracting Government to provide protection against the threat.

COMPANY SECURITY OFFICER

The Company shall designate a company security officer. A person designated as the company security officer may act as the company security officer for one or more ships, depending on the number or types of ships the Company operates provided it is clearly identified for which ships this person is responsible. A Company may, depending on the number or types of ships they operate designate several persons as company security officers provided it is clearly identified for which ships each person is responsible.

In addition to those specified elsewhere in ISPS Code, the duties and responsibilities of the company security officer shall include, but are not limited to:

.1 advising the level of threats likely to be encountered by the ship, using appropriate security assessments and other relevant information;

.2 ensuring that ship security assessments are carried out;

.3 ensuring the development, the submission for approval, and thereafter the implementation and maintenance of the ship security plan;

.4 ensuring that the ship security plan is modified, as appropriate, to correct deficiencies and satisfy the security requirements of the individual ship;

.5 arranging for internal audits and reviews of security activities;

.6 arranging for the initial and subsequent verifications of the ship by the Administration or the recognized security organization;

.7 ensuring that deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance are promptly addressed and dealt with;

.8 enhancing security awareness and vigilance;

.9 ensuring adequate training for personnel responsible for the security of the ship;

.10 ensuring effective communication and co-operation between the ship security officer and the relevant port facility security officers;

.11 ensuring consistency between security requirements and safety requirements;

.12 ensuring that, if sister-ship or fleet security plans are used, the plan for each ship reflects the ship-specific information accurately; and

.13 ensuring that any alternative or equivalent arrangements approved for a particular

ship or group of ships are implemented and maintained.

SHIP SECURITY OFFICER

A ship security officer shall be designated on each ship. In addition to those specified elsewhere in the Code, the duties and responsibilities of the ship security officer shall include, but are not limited to:

.1 undertaking regular security inspections of the ship to ensure that appropriate security measures are maintained;

.2 maintaining and supervising the implementation of the ship security plan, including any amendments to the plan;

.3 coordinating the security aspects of the handling of cargo and ship.s stores with other shipboard personnel and with the relevant port facility security officers;

.4 proposing modifications to the ship security plan;

.5 reporting to the company security officer any deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance and implementing any corrective actions;

.6 enhancing security awareness and vigilance on board;

.7 ensuring that adequate training has been provided to shipboard personnel, as appropriate;

.8 reporting all security incidents;

.9 co-ordinating implementation of the ship security plan with the company security officer and the relevant port facility security officer; and

.10 ensuring that security equipment is properly operated, tested, calibrated and maintained, if any.

P ORT FACILITY SECURITY

A port facility is required to act upon the security levels set by the Contracting Government within whose territory it is located. Security measures and procedures shall be applied at the port facility in such a manner as to cause a minimum of interference with, or delay to, passengers, ship, ship.s personnel and visitors, goods and services.

At security level 1, the following activities shall be carried out through appropriate measures in all port facilities, taking into account the guidance given in part B of ISPS Code, in order to identify and take preventive measures against security incidents:

.1 ensuring the performance of all port facility security duties;
.2 controlling access to the port facility;
.3 monitoring of the port facility, including anchoring and berthing area(s);
.4 monitoring restricted areas to ensure that only authorized persons have access;
.5 supervising the handling of cargo;

.6 supervising the handling of ship.s stores; and
.7 ensuring that security communication is readily available.

At security level 2, the additional protective measures, specified in the port facility security plan, shall be implemented for each activity detailed in section 14.2, taking into account the guidance given in part B of ISPS Code. At security level 3, further specific protective measures, specified in the port facility security plan, shall be implemented for each activity detailed in section 14.2, taking into account the guidance given in part B of ISPS Code. In addition, at security level 3, port facilities are required to respond to and implement any security instructions given by the Contracting Government within whose territory the port facility is located.

When a port facility security officer is advised that a ship encounters difficulties in complying with the requirements of chapter XI-2 or this part or in implementing the appropriate measures and procedures as detailed in the ship security plan, and in the case of security level 3 following any security instructions given by the Contracting Government within whose territory the port facility is located, the port facility security officer and ship security officer shall liase and co-ordinate appropriate actions. When a port facility security officer is advised that a ship is at a security level, which is higher than that of the port facility, the port facility security officer shall report the matter to the competent authority and shall liase with the ship security officer and co-ordinate appropriate actions, if necessary.

PORT FACILITY SECURITY OFFICER

A port facility security officer shall be designated for each port facility. A person may be designated as the port facility security officer for one or more port facilities. In addition to those specified elsewhere in ISPS Code, the duties and responsibilities of the port facility security officer shall include, but are not limited to:

.1 conducting an initial comprehensive security survey of the port facility taking into account the relevant port facility security assessment;
.2 ensuring the development and maintenance of the port facility security plan;
.3 implementing and exercising the port facility security plan;
.4 undertaking regular security inspections of the port facility to ensure the continuation of appropriate security measures;
.5 recommending and incorporating, as appropriate, modifications to the port facility security plan in order to correct deficiencies and to update the plan to take into account of relevant changes to the port facility;
.6 enhancing security awareness and vigilance of the port facility personnel;
.7 ensuring adequate training has been provided to personnel responsible for the security of the port facility;
.8 reporting to the relevant authorities and maintaining records of occurrences which threaten the security of the port facility;
.9 co-ordinating implementation of the port facility security plan with the appropriate Company and ship security officer(s);
.10 co-ordinating with security services, as appropriate;
.11 ensuring that standards for personnel responsible for security of the port facility are met;
.12 ensuring that security equipment is properly operated, tested, calibrated and maintained, if any; and
.13 assisting ship security officers in confirming the identity of those seeking to board

the ship when requested.
17.3 The port facility security officer shall be given the necessary support to fulfil the duties and responsibilities imposed by chapter XI-2 and this Part of the Code.

Vessel Personnel with Specific Security Duties

Existing protective measures and procedures in practice, including inspection, control and monitoring equipment, personnel identification documents and communication, alarm, lighting, access control and other appropriate systems.

On-scene security surveys

Oon-scene security survey is an integral part of any Vessel Security Assessment. They should understand that the survey should fulfil the following functions:

 identification of existing security measures, procedures and operations;
 identification and evaluation of key vessel operations that it is important to protect;
 identification of possible threats to the key vessel operations and the likelihood of their occurrence, in order to establish and prioritize security measures; and
 identification of weaknesses, including human factors in the infrastructure, policies and procedures.

It should be emphasized to course participants that the on-scene survey should examine and evaluate
existing vessel protective measures, procedures and operations for:

 ensuring the performance of all security duties;
 controlling access to the vessel, through the use of identification systems or otherwise;
 controlling the embarkation of vessel personnel and other persons and their effects, including personal effects and baggage whether accompanied or unaccompanied;
 supervising the handling of cargo and the delivery of vessel stores;
 monitoring restricted areas to ensure that only authorized persons have access;
 monitoring deck areas and areas surrounding the vessel; and
 ensuring the ready availability of security communications, information, and equipment.

Chapter 4

Vessel Security Assessment

SHIP SECURITY ASSESSMENT

The ship security assessment is an essential and integral part of the process of developing and updating the ship security plan. The company security officer shall ensure that the ship security assessment is carried out by persons with appropriate skills to evaluate the security of a ship, in accordance with this ISPS Guidelines. A recognized security organization may be authorized by administration to carry out the ship security assessment of a specific ship. The ship security assessment shall be documented, reviewed, accepted and retained by the Company.The ship security assessment shall include an on-scene security survey and, at least, the
following elements:

.1 identification of existing security measures, procedures and operations;

.2 identification and evaluation of key ship board operations that it is important to protect;

.3 identification of possible threats to the key ship board operations and the likelihood of their occurrence, in order to establish and prioritise security measures; and

.4 identification of weaknesses, including human factors in the infrastructure, policies and procedures.

Assessment tools

Trainees must be encouraged to adopt systematic and consistent approaches to the evaluation of security conditions and vulnerabilities. Vessel personnel with specific security duties may be called upon to assist in these evaluations. The use of checklists to perform assessments of security in day-to-day operations should therefore be discussed, noting the inclusion of categories such as the following:

 General layout of the vessel.
 Location of areas that should have restricted access, such as the bridge, engine room, radio room,
etc.
 Location and function of each actual or potential access point to the vessel.
 Open deck arrangement including the height of the deck above water.
 Emergency and stand-by equipment available to maintain essential services.
 Numerical strength, reliability, and security duties of the vessel's crew.
 Existing security and safety equipment for protecting the passengers and crew.
 Existing agreements with private security companies for providing vessel and waterside security services.

 Existing protective measures and procedures in practice, including inspection, control and monitoring equipment, personnel identification documents and communication, alarm, lighting, access control and other appropriate systems.

On-scene security surveys

On-scene security survey is an integral part of any Vessel Security Assessment. The survey should fulfill the following functions:

 identification of existing security measures, procedures and operations;
 identification and evaluation of key vessel operations that it is important to protect;
 identification of possible threats to the key vessel operations and the likelihood of their occurrence, in order to establish and prioritize security measures; and
 identification of weaknesses, including human factors in the infrastructure, policies and procedures. It should be emphasized to course participants that the on-scene survey should examine and evaluate existing vessel protective measures, procedures and operations for:
 ensuring the performance of all security duties;
 controlling access to the vessel, through the use of identification systems or otherwise;
 controlling the embarkation of vessel personnel and other persons and their effects, including personal effects and baggage whether accompanied or unaccompanied;
 supervising the handling of cargo and the delivery of vessel stores;
 monitoring restricted areas to ensure that only authorized persons have access;
 monitoring deck areas and areas surrounding the vessel; and
 ensuring the ready availability of security communications, information, and equipment.

Chapter 5

SHIP SECURITY PLAN

Each ship shall carry on board a ship security plan approved by the Administration. The plan shall make provisions for the three security levels as defined in ISPS Code. The Administration may entrust the review and approval of ship security plans, or of amendments to a previously approved plan, to recognized security organizations. In such cases the recognized security organization, undertaking the review and approval of a ship security plan, or its amendments, for a specific ship shall not have been involved in either the preparation of the ship security assessment or of the ship security plan, or of the amendments, under review.

The submission of a ship security plan, or of amendments to a previously approved plan,for approval shall be accompanied by the security assessment on the basis of which the plan, or the amendments, have been developed. Such a plan shall be developed**,** taking into account the guidance given in part B of ISPS Code and shall be written in the working language or languages of the ship. If the language or languages used is not English, French or Spanish, a translation into one of these languages shall be included. The plan shall address, at least, the following:

.1 measures designed to prevent weapons, dangerous substances and devices intended for use against persons, ships or ports and the carriage of which is not authorized from being taken on board the ship;

.2 identification of the restricted areas and measures for the prevention of unauthorized access to them;

.3 measures for the prevention of unauthorized access to the ship;

.4 procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface;

.5 procedures for responding to any security instructions Contracting Governments may give at security level 3;

.6 procedures for evacuation in case of security threats or breaches of security;

.7 duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects;

.8 procedures for auditing the security activities;

.9 procedures for training, drills and exercises associated with the plan;

.10 procedures for interfacing with port facility security activities;

.11 procedures for the periodic review of the plan and for updating;

.12 procedures for reporting security incidents;

.13 identification of the ship security officer;

.14 identification of the company security officer including 24-hour contact details;

.15 procedures to ensure the inspection, testing, calibration, and maintenance of any security equipment provided on board;

.16 frequency for testing or calibration of any security equipment provided on board;

.17 identification of the locations where the ship security alert system activation points are provided;1 and

.18 procedures, instructions and guidance on the use of the ship security alert system, including the testing, activation, deactivation and resetting and to limit false alerts.1

9.4.1 Personnel conducting internal audits of the security activities specified in the plan or evaluating its implementation shall be independent of the activities being audited unless this is impracticable due to the size and the nature of the Company or of the ship.

9.5 The Administration shall determine which changes to an approved ship security plan or to any security equipment specified in an approved plan shall not be implemented unless the relevant amendments to the plan are approved by the Administration. Any such changes shall be at least as effective as those measures prescribed in chapter XI-2 and this Part of the Code.

9.5.1 The nature of the changes to the ship security plan or the security equipment that have been specifically approved by the Administration, pursuant to section 9.5, shall be documented in a manner that clearly indicates such approval. This approval shall be available on board and shall be presented together with the International Ship Security Certificate (or the Interim International Ship Security Certificate). If these changes are temporary, once the original approved measures or equipment are reinstated, this documentation no longer needs to be retained by the ship.

The plan may be kept in an electronic format. In such a case, it shall be protected by procedures aimed at preventing its unauthorized deletion, destruction or amendment. The plan shall be protected from unauthorized access or disclosure. Ship security plans are not subject to inspection by officers duly authorized by a Contracting Government to carry out control and compliance measures in accordance with regulation XI-2/9

Administrations may allow, in order to avoid compromising in any way the objective of providing on board the ship security alert system, this information to be kept elsewhere on board in a document known to the master, the ship security officer and other senior shipboard personnel as may be decided by the Company.

If the officers duly authorized by a Contracting Government have clear grounds to believe that the ship is not in compliance with the requirements of chapter XI-2 or part A of ISPS Code, and the only means to verify or rectify the non-compliance is to review the relevant requirements of the ship security plan, limited access to the specific sections of the plan relating to the noncompliance is exceptionally allowed, but only with the consent of the Contracting Government of, or the master of, the ship concerned. Nevertheless, the provisions in the plan relating to section 9.4 subsections .2, .4, .5, .7, .15, .17 and .18 of this Part of the Code are considered as confidential information, and cannot be subject to inspection unless otherwise agreed by the Contracting Governments concerned.

Chapter 6

Security Equipment

Security equipment and systems

security equipment and systems that are useful in enhancing maritime security, both ashore and afloat. Examples of such equipment include:

- AIS
- Vessel Security Alert System
- Locks
- Lighting
- Handheld radios
- GMDSS equipment
- Closed Circuit Televisions
- Automatic Intrusion Detection Device (Burglar Alarm)
- Metal detectors
- Explosive detectors
- Baggage screening equipment
- Container X-ray devices
- General alarm

Anatomy of a Metal Detector

A typical metal detector is light-weight and consists of just a few parts:

1. **Stabilizer** (optional) - used to keep the unit steady as you sweep it back and forth
2. **Control box** - contains the circuitry, controls, speaker, batteries and the microprocessor
3. **Shaft** - connects the control box and the coil; often adjustable so you can set it at a comfortable level for your height
4. **Search coil** - the part that actually senses the metal; also known as the "search head," "loop" or "antenna"

Most systems also have a **jack** for connecting headphones, and some have the control box below the shaft and a small **display unit** above.

Operating a metal detector is simple. Once you turn the unit on, you move slowly over the area you wish to search. In most cases, you sweep the coil (search head) back and forth over the ground in front of you. When you pass it over a target object, an audible signal occurs. More advanced metal detectors provide displays that pinpoint the type of metal it has detected and how deep in the ground the target object is located.

Metal detectors use one of three technologies:

- **Very low frequency** (VLF)
- **Pulse induction** (PI)
- **Beat-frequency oscillation** (BFO)

Ship Security Alert System (SSAS) is part of the ISPS code and is a system that contributes to the International Maritime Organization's (IMO)'s efforts to strengthen maritime security and suppress acts of terrorism and piracy against shipping. The system is a joint project between Cospas-Sarsat and the IMO. In case of attempted piracy or terrorism, the ship's SSAS beacon can be activated, and appropriate law-enforcement or military forces can be dispatched. An SSAS beacon operates with similar principles to the aircraft transponder emergency code 7700.

When an SSAS alert is triggered: [1]

- the Rescue Coordination Centres (RCCs) or SAR Points of Contact (SPOCs) for the country code the beacon is transmitting is notified discreetly
- national authorities dispatch appropriate forces to deal with the terrorist or pirate threat

Operational limitations of security equipment and systems

The functional limitations and operating constraints of security equipment that they may encounter are effective range, environmental sensitivities, and operator (human) error should be addressed as appropriate. Personnel using security equipment must familiarize themselves with the manufactures operation instruction including the limitations on use.

Testing, calibration and maintenance of security equipment and systems

Personnel should be familiar with methods for ensuring the continuing accuracy, efficiency, and operational readiness of selected items of security equipment and associated systems.

Chapter 7

Threat Identification, Recognition, and Response

Methods of physical searches and non-intrusive inspections

Unless there are clear security grounds for doing so; members of the vessel's crew should not be required to search their colleagues or their personal effects. It should be conveyed that any such search shall be undertaken in a manner that fully takes into account the human rights of the individual and preserves his or her basic human dignity.

Execution and coordination of searches

Personnel on board must acquainted themselves with the utility of "check cards" in conducting systematic searches. A "check card" is a card that can be issued to each searcher specifying the route to follow and the areas to be searched. These cards can be colour-coded for different areas of responsibility, for example blue for deck, red for engine room. On completion of individual search tasks, the cards are returned to a central control point. When all cards are returned, the search is known to be complete. The findings of the search can then be discussed. Course participants should be familiar with the list of basic equipment that may be employed in conducting searches. This list may include:

 flashlights and batteries;

 screwdrivers, wrenches and crowbars;

 mirrors and probes;

 gloves, hard hats, overalls and non-slip footwear;

 plastic bags and envelopes for collection of evidence;

 forms on which to record activities and discoveries. Personnel on board ship should learn procedures to be followed so as to ensure effective and efficient searches.

 Crew members should not be allowed to search their own areas in recognition of the possibility that they may have concealed packages or devices in their own work or personal areas

 The search should be conducted according to a specific plan or schedule and must be carefully controlled.

 Special consideration should be given to search parties working in pairs with one searching "high" and one searching "low". If a suspicious object is found, one of the pair can remain on guard while the other reports the find.

 Searchers should be able to recognize suspicious items.

 There should be a system for marking or recording "clean" areas

 Searchers should maintain contact with the search controllers, perhaps by UHF / VHF radio, bearing in mind the dangers of using radio equipment in the vicinity of Improvised Explosive Devices (IEDs).

 Searchers should have clear guidance on what to do if a suspect package, device, or situation is found.

 Searchers should bear in mind that weapons and other dangerous devices may be intentionally placed to match its context as a means of disguise, such as a toolbox in an engine room. Participants in the course should be acquainted with the fact that there are many places on board a vessel where weapons, dangerous substances, and devices can be concealed. Some of these are:

Cabins

 Back sides and underneath drawers

 Between bottom drawer and deck

 Beneath bunks, e.g. taped to bunk frame under mattress

 Under wash basin

 Behind removable medicine chest

 Inside radios, recorders etc.

 Ventilator ducts

 Inside heater units

 Above or behind light fixtures

 Above ceiling and wall panels

 Cutouts behind bulkheads, pictures, etc.

 False bottom clothes closets-hanging clothes

 Inside wooden clothes hangers

 Inside rolled socks, spare socks

 Hollowed-out molding

Companionways

 Ducts

 Wire harnesses

 Railings

 Fire extinguishers

 Fire hoses and compartments

 Access panels in floors, walls, ceilings

 Behind or inside water coolers, igloos

Toilet and Showers

- Behind and under sinks
- Behind toilets
- In ventilation ducts and heaters
- Toilet tissue rollers, towel dispensers, supply lockers
- Taped to shower curtains, exposed piping, and light fixtures
- Access panels in floors, walls, ceiling

Deck

- Ledges on deck housing, electrical switch rooms, winch control panels
- Lifeboat storage compartments, under coiled lines, in deck storage rooms
- Paint cans, cargo holds, battery rooms, chain lockers.

Engine room

- Under deck plates
- Cofferdams, machinery pedestals, bilges
- Journal-bearing shrouds and sumps on propeller shaft
- Under catwalk, in bilges, in shaft alley
- Escape ladders and ascending area.
- In ventilation ducts, attached to piping or in tanks with false gauges.
- Equipment boxes, emergency steering rooms, storage spaces.

Galleys and Stewards' Stores

- Flour bins and dry stores
- Vegetable sacks, canned foods (re-glued labels)
- Under or behind standard refrigerators
- Inside fish or sides of beef in freezers
- Bonded store lockers, slop chest, storage rooms.

Recognition, on a non-discriminatory basis, of persons posing potential security risks

Personnel should recognise suspicious patterns of behavior, and avoid racial profiling and ethnic stereotyping. Examples of suspicious behaviours include:

- Unknown persons photographing vessels or facilities.
- Unknown persons attempting to gain access to vessels or facilities.

 Individuals establishing businesses or roadside food stands either adjacent or in proximity to facilities.

 Unknown persons loitering in the vicinity of vessels or port facilities for extended periods of time.

 Vehicles with personnel in them loitering and perhaps taking photographs or creating diagrams of vessels or facilities.

 Small boats with personnel on board loitering and perhaps taking photographs or creating diagrams of vessels or facilities.

 General aviation aircraft operating in proximity to vessels or facilities.

 Persons who may be carrying bombs or participating in suicide squad activities.

 Unknown persons attempting to gain information about vessels or facilities by walking up to personnel or their families and engaging them in a conversation.

 Vendors attempting to sell merchandise.

 Workmen trying to gain access to vessels to repair, replace, service, or install equipment.

 E-mails attempting to obtain information regarding vessels, personnel, or standard operating procedures.

 Package drop-offs/attempted drop-offs.

 Anti-national sentiments being expressed by employees or vendors.

 Anti-national pamphlets or flyers distributed to employees or placed on windshields in parking lots.

 Out-of-the-ordinary phone calls.

 Recreational boaters or persons aboard refugee craft posing as mariners in distress to attract assistance from other vessels.

Techniques used to circumvent security measures

No security equipment or measure is infallible. There are techniques that can be employed to evade security systems and controls, such as the disabling of alarm systems, picking of locks, jamming of radio signals, etc.

Chapter 8

Emergency Preparedness Security drills and exercises

Vessel Security Actions

Action to be taken onboard ship will vary depending upon the prevalent security threat and what is the Security level.

Actions required by different security levels

The basic guideline sfor actions to be taken are given in ISPS Code. The actions for a particular ship are given in the Ship Security plan. Based on these, the ships will prepare their check lists for each security level to ensure that no action is overlooked for implementation.

Maintaining security of the vessel/port interface

The vessel/port interface determines the need for a Facility Security Plan and the interaction with the Vessel Security Plan. Instructors should ensure that trainees are clear on the critical importance of the interaction between the vessel security plan and that of the facility.

DECLARATION OF SECURITY

Contracting Governments shall determine when a Declaration of Security is required by assessing the risk the ship/port interface or ship to ship activity poses to persons, property or the environment. A ship can request completion of a Declaration of Security when:

.1 the ship is operating at a higher security level than the port facility or another ship it is interfacing with;
.2 there is an agreement on a Declaration of Security between Contracting Governments covering certain international voyages or specific ships on those voyages;
.3 there has been a security threat or a security incident involving the ship or involving the port facility, as applicable;
.4 the ship is at a port which is not required to have and implement an approved port facility security plan; or
.5 the ship is conducting ship to ship activities with another ship not required to have and implement an approved ship security plan.
5.3 Requests for the completion of a Declaration of Security, under this section, shall be acknowledged by the applicable port facility or ship.
5.4 The Declaration of Security shall be completed by:
.1 the master or the ship security officer on behalf of the ship(s); and, if appropriate,
.2 the port facility security officer or, if the Contracting Government determines otherwise, by any other body responsible for shore-side security, on behalf of the port facility.

The Declaration of Security shall address the security requirements that could be shared between a port facility and a ship (or between ships) and shall state the responsibility for each. Contracting Governments shall specify**,** bearing in mind the provisions of regulation XI-2/9.2.3, the minimum period for which Declarations of Security shall be kept by the port facilities located within their territory. Administrations shall specify, bearing in mind the provisions of regulation XI-2/9.2.3, the minimum period for which Declarations of Security shall be kept by ships entitled to fly their flag.

Execution of security procedures

Building on the understanding gained from previous sections in this course, trainees should be ready to synthesize the requirements and plans into actual procedures such as security inspections, controlling access to the vessel, verifying and controlling the use of identification credentials, monitoring deck areas and areas surrounding the vessel, and so forth.

Execution of contingency plans

Variety of contingencies associated with terrorism and other criminal activities that may arise in the maritime setting. Possible responses in the case of bomb threats, explosions, piracy, hijackings, and similar events are included in the SSP.

Security drills and exercises

Tthe objective of drills and exercises is to ensure that vessel personnel are proficient in all assigned security duties at all security levels and in the identification of any security-related deficiencies that need to be addressed. Personnel on board ship should learn that effective implementation of the provisions of the Vessel Security Plan requires that drills be conducted at least once every three months.

In addition, in cases where more than 25 percent of the vessel's personnel have been changed, at any one time, with personnel that have not previously participated in any drill on that vessel within the last 3 months, a drill should be conducted within one week of the change. These drills should test individual elements of the plan such as:

- damage to, or destruction of, the vessel or of a port facility, e.g. by explosive devices, arson, sabotage or vandalism;
- hijacking or seizure of the vessel or of persons on board;
- tampering with cargo, essential vessel equipment, systems, or vessel stores;
- unauthorized access or use, including presence of stowaways;
- smuggling weapons or equipment, including weapons of mass destruction;
- use of the vessel to carry persons intending to cause a security incident, or their equipment;
- use of the vessel itself as a weapon or as a means to cause damage or destruction;
- attacks from seaward while at berth or at anchor; and
- attacks while at sea.

Various types of exercises involving participation of vessel security personnel should be carried out at least once each calendar year with no more than 18 months between the exercises. These exercises should test communications, coordination, resource availability, and response. These exercises may be:

- full scale or live;
- tabletop simulation or seminar; or
- combined with other exercises held such as search and rescue or emergency response exercises.

Chapter 9

Ship Security Action

Access to the ship

The SSP should establish the security measures covering all means of access to the ship identified in the SSA. This should include any:

.1 access ladders;
.2 access gangways;
.3 access ramps;
.4 access doors, side scuttles, windows and ports;
.5 mooring lines and anchor chains; and
.6 cranes and hoisting gear.

For each of these the SSP should identify the appropriate locations where access restrictions or prohibitions should be applied for each of the security levels. For each security level the SSP should establish the type of restriction or prohibition to be applied and the means of enforcing them.

The SSP should establish for each security level the means of identification required to allow access to the ship and for individuals to remain on the ship without challenge, this may involve developing an appropriate identification system allowing for permanent and temporary identifications, for ship.s personnel and visitors respectively. Any ship identification system should, when it is practicable to do so, be co-ordinated with that applying to the port facility.

Passengers should be able to prove their identity by boarding passes, tickets, etc., but should not be permitted access to restricted areas unless supervised. The SSP should establish provisions to ensure that the identification systems are regularly updated, and that abuse of procedures should be subject to disciplinary action.

Those unwilling or unable to establish their identity and/or to confirm the purpose of their visit when requested to do so should be denied access to the ship and their attempt to obtain access should be reported, as appropriate, to the SSOs, the CSOs, the Port Facility Security Officer (PFSO) and to the national or local authorities with security responsibilities.

The SSP should establish the frequency of application of any access controls particularly if they are to be applied on a random, or occasional, basis.

Security Level 1
At security level 1, the SSP should establish the security measures to control access to the ship, where the following may be applied:
.1 checking the identity of all persons seeking to board the ship and confirming their reasons for doing so by checking, for example, joining instructions, passenger tickets, boarding passes, work orders etc;

.2 in liaison with the port facility the ship should ensure that designated secure areas are established in which inspections and searching of persons, baggage (including carry on items), personal effects, vehicles and their contents can take place;

.3 in liaison with the port facility the ship should ensure that vehicles destined to be loaded on board car carriers, ro-ro and other passenger ships are subjected to search prior to loading, in accordance with the frequency required in the SSP;

.4 segregating checked persons and their personal effects from unchecked persons and their personal effects;

.5 segregating embarking from disembarking passengers;

.6 identification of access points that should be secured or attended to prevent unauthorized access;

.7 securing, by locking or other means, access to unattended spaces adjoining areas to which passengers and visitors have access; and

.8 providing security briefings to all ship personnel on possible threats, the procedures for reporting suspicious persons, objects or activities and the need for vigilance.

At security level 1, all those seeking to board a ship should be liable to search. The frequency of such searches, including random searches, should be specified in the approved SSP and should be specifically approved by the Administration. Such searches may best be undertaken by the port facility in close co-operation with the ship and in close proximity to it. Unless there are clear security grounds for doing so, members of the ship.s personnel should not be required to search their colleagues or their personal effects. Any such search shall be undertaken in a manner which fully takes into account the human rights of the individual and preserves their basic human dignity.

Security Level 2

At security level 2, the SSP should establish the security measures to be applied to protect against a heightened risk of a security incident to ensure higher vigilance and tighter control, which may include:

.1 assigning additional personnel to patrol deck areas during silent hours to deter unauthorized access;
.2 limiting the number of access points to the ship, identifying those to be closed and the means of adequately securing them;
.3 deterring waterside access to the ship, including**,** for example, in liaison with the port facility, provision of boat patrols;
.4 establishing a restricted area on the shore-side of the ship, in close co-operation

with the port facility;
.5 increasing the frequency and detail of searches of persons, personal effects, and vehicles being embarked or loaded onto the ship;
.6 escorting visitors on the ship;
.7 providing additional specific security briefings to all ship personnel on any identified threats, re-emphasising the procedures for reporting suspicious persons, objects, or activities and the stressing the need for increased vigilance; and
.8 carrying out a full or partial search of the ship.

Security Level 3

At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:

.1 limiting access to a single, controlled, access point;
.2 granting access only to those responding to the security incident or threat thereof;
.3 directions of persons on board;
.4 suspension of embarkation or disembarkation;
.5 suspension of cargo handling operations, deliveries etc;
.6 evacuation of the ship;
.7 movement of the ship; and
.8 preparing for a full or partial search of the ship.

Restricted areas on the ship

The SSP should identify the restricted areas to be established on the ship, specify their extent, times of application, the security measures to be taken to control access to them and those to be taken to control activities within them. The purpose of restricted areas are to:

.1 prevent unauthorized access;

.2 protect passengers, ship's personnel, and personnel from port facilities or other agencies authorized to be on board the ship;

.3 protect sensitive security areas within the ship; and

.4 protect cargo and ship's stores from tampering.

The SSP should ensure that there are clearly established policies and practices to control access to all restricted areas them.
The SSP should provide that all restricted areas should be clearly marked indicating that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security.

Restricted areas may include:

.1 navigation bridge, machinery spaces of category A and other control stations as defined in chapter II-2;

.2 spaces containing security and surveillance equipment and systems and their controls and lighting system controls;

.3 ventilation and air-conditioning systems and other similar spaces;

.4 spaces with access to potable water tanks, pumps, or manifolds;

.5 spaces containing dangerous goods or hazardous substances;

.6 spaces containing cargo pumps and their controls;

.7 cargo spaces and spaces containing ship.s stores;

.8 crew accommodation; and

.9 any other areas as determined by the CSO, through the SSA to which access must be restricted to maintain the security of the ship.

Chapter 10

Security Administration

Training, drills and exercises on ship security

The company security officer and appropriate shore-based personnel shall have knowledge and have received training, taking into account the guidance given in part B of this Code. The ship security officer shall have knowledge and have received training, taking into account the guidance given in part B of this Code.Shipboard personnel having specific security duties and responsibilities shall understand their responsibilities for ship security as described in the ship security plan and shall have sufficient knowledge and ability to perform their assigned duties, taking into account the guidance given in part B of this Code. To ensure the effective implementation of the ship security plan, drills shall be carried out at appropriate intervals taking into account the ship type, ship personnel changes, port facilities to be visited and other relevant circumstances, taking into account the guidance given in part B of this Code.The company security officer shall ensure the effective coordination and implementation of ship security plans by participating in exercises at appropriate intervals, taking into account the guidance given in part B of this Code.

Records of the following activities addressed in the ship security plan shall be kept on board for at least the minimum period specified by the Administration, bearing in mind the provisions of regulation XI-2/9.2.3:

.1 training, drills and exercises;
.2 security threats and security incidents;
.3 breaches of security;
.4 changes in security level;
.5 communications relating to the direct security of the ship such as specific threats to the ship or to port facilities the ship is, or has been;
.6 internal audits and reviews of security activities;
.7 periodic review of the ship security assessment;
.8 periodic review of the ship security plan;
.9 implementation of any amendments to the plan; and
.10 maintenance, calibration and testing of any security equipment provided on board including testing of the ship security alert system.

The records shall be kept in the working language or languages of the ship. If the language or languages used are not English, French or Spanish, a translation into one of these languages shall be included. The records may be kept in an electronic format. In such a case, they shall be protected by procedures aimed at preventing their unauthorized deletion, destruction or amendment. The records shall be protected from unauthorized access or disclosure.

Form of the International Ship Security Certificate

INTERNATIONAL SHIP SECURITY CERTIFICATE

(official seal) *(State)*

Certificate Number

Issued under the provisions of the

INTERNATIONAL CODE FOR THE SECURITY OF SHIPS AND OF PORT FACILITIES (ISPS CODE)

Under the authority of the Government of _____
(name of State)

by

(persons or organization authorized)

Name of ship :.....
Distinctive number or letters :.....
Port of registry :.....
Type of ship :.....
Gross tonnage :.....
IMO Number :.....
Name and address of the Company :.....

THIS IS TO CERTIFY:

1 that the security system and any associated security equipment of the ship has been verified in accordance with section 19.1 of part A of the ISPS Code;

2 that the verification showed that the security system and any associated security equipment of the ship is in all respects satisfactory and that the ship complies with the applicable requirements of chapter XI-2 of the Convention and part A of the ISPS Code;

3 that the ship is provided with an approved Ship Security Plan.

Date of initial / renewal verification on which this certificate is based.....

This Certificate is valid until .....
subject to verifications in accordance with section 19.1.1 of part A of the ISPS Code.

Issued at .....
(place of issue of the Certificate)

Date of issue ....
(signature of the duly authorized official issuing the Certificate)

(Seal or stamp of issuing authority, as appropriate)

ENDORSEMENT FOR INTERMEDIATE VERIFICATION

THIS IS TO CERTIFY that at an intermediate verification required by section 19.1.1 of part A of the ISPS Code the ship was found to comply with the relevant provisions of chapter XI-2 of the Convention and part A of the ISPS Code.

Intermediate verification

Signed .....
(Signature of authorized official)
Place .....

Date .....

(Seal or stamp of the authority, as appropriate)

ENDORSEMENT FOR ADDITIONAL VERIFICATIONS[1]

Additional verification

Signed .....
(Signature of authorized official)
Place .....

Date .....

(Seal or stamp of the authority, as appropriate)

Additional verification

Signed .....
(Signature of authorized official)
Place .....

Date .....

(Seal or stamp of the authority, as appropriate)

Additional verification

Signed .....
(Signature of authorized official)
Place .....

Date .....

(Seal or stamp of the authority, as appropriate)

1 This part of the certificate shall be adapted by the Administration to indicate whether it has established additional verifications as provided for in section 19.1.1.4.

ADDITIONAL VERIFICATION IN ACCORDANCE WITH SECTION A/19.3.7.2 OF **THE ISPS CODE**

THIS IS TO CERTIFY that at an additional verification required by section 19.3.7.2 of part A of the ISPS Code the ship was found to comply with the relevant provisions of chapter XI-2 of the Convention and part A of the ISPS Code.

Signed .....
(Signature of authorized official)
Place .....

Date .....

(Seal or stamp of the authority, as appropriate)

ENDORSEMENT TO EXTEND THE CERTIFICATE IF VALID FOR LESS THAN 5 **YEARS** WHERE SECTION **A/19.3.3 OF THE ISPS CODE APPLIES**

The ship complies with the relevant provisions of part A of the ISPS Code, and the Certificate shall, in accordance with section 19.3.3 of part A of the ISPS Code, be accepted as valid until

Signed .....
(Signature of authorized official)
Place .....

Date .....

(Seal or stamp of the authority, as appropriate)

ENDORSEMENT WHERE THE RENEWAL VERIFICATION HAS BEEN COMPLETED AND SECTION A/*19.3.4* **OF THE ISPS CODE APPLIES**

The ship complies with the relevant provisions of part A of the ISPS Code, and the Certificate shall, in accordance with section 19.3.4 of part A of the ISPS Code, be accepted as valid until

Signed .....
(Signature of authorized official)
Place .....

Date .....

(Seal or stamp of the authority, as appropriate)

ENDORSEMENT TO EXTEND THE VALIDITY OF THE CERTIFICATE UNTIL REACHING THE PORT **OF VERIFICATION WHERE SECTION A/19.3.5** OF **THE ISPS CODE APPLIES OR FOR A PERIOD OF GRACE WHERE SECTION A/19.3.6 OF THE ISPS CODE APPLIES**

This Certificate shall, in accordance with section 19.3.5 / 19.3.6 of part A of the ISPS Code, be accepted as valid until .....

Signed .....
(Signature of authorized official) Place .....

Date .....

(Seal or stamp of the authority, as appropriate)

ENDORSEMENT FOR ADVANCEMENT OF EXPIRY DATE WHERE SECTION A/19.3.7.1 OF THE ISPS CODE APPLIES

In accordance with section 19.3.7.1 of part A of the ISPS Code, the new expiry date2 is

Signed .....
(Signature of authorized official) Place .....

Date .....

(Seal or stamp of the authority, as appropriate)

APPENDIX 2

Form of the Interim International Ship Security Certificate

INTERIM INTERNATIONAL SHIP SECURITY CERTIFICATE

(official seal) *(State)*

Certificate No.

Issued under the provisions of the

INTERNATIONAL CODE FOR THE SECURITY OF SHIPS AND OF PORT FACILITIES

Delete as appropriate.
In case of completion of this part of the certificate the expiry date shown on the front of the certificate shall also be amended accordingly.

(ISPS CODE)

Under the authority of the Government of _____
(name of State)

by_____
(persons or organization authorized)

Name of ship :.....
Distinctive number or letters : .....
Port of registry :.....
Type of ship :.....
Gross tonnage :.....
IMO Number :.....
Name and address of company : .....
Is this a subsequent, consecutive interim certificate? Yes/ No
If Yes, date of issue of initial interim certificate.....

THIS IS TO CERTIFY THAT the requirements of section A/19.4.2 of the ISPS Code have been complied with.

This Certificate is issued pursuant to section A/19.4 of the ISPS Code.

This Certificate is valid until.....

Issued at.....
(place of issue of the certificate)

Date of issue..... .....
(signature of the duly authorized official issuing the Certificate)

(Seal or stamp of issuing authority, as appropriate)

*

Delete as appropriate

Chapter 11

Introduction to Ship Piracy

Piracy at sea is a worldwide phenomenon which has affected not only the coasts of Africa, but also Indonesia, Malaysia, the Philippines, Yemen, and Venezuela. American citizens considering travel by sea should exercise caution when near and within these coastal areas. The following definition of piracy is contained in article 101 of the 1982 United Nations Convention on the Law of the Sea (UNCLOS):

"Piracy consists of any of the following acts:

(a) any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed:
   (i) on the high seas, against another ship or aircraft, or against persons or property on board such ship
   or aircraft;
   (ii) against a ship, aircraft, persons or property in a place outside the jurisdiction of any State;
(b) any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft;
© any act inciting or of intentionally facilitating an act described in sub-paragraph (a) or (b)."

Piracy at sea is a worldwide phenomenon which has affected not only the coasts of Africa, but also Indonesia, Malaysia, the Philippines, Yemen, and Venezuela. American citizens considering travel by sea should exercise caution when near and within these coastal areas. The following definition of piracy is contained in article 101 of the 1982 United Nations Convention on the Law of the Sea (UNCLOS):

"Piracy consists of any of the following acts:

(a) any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed:
   (i) on the high seas, against another ship or aircraft, or against persons or property on board such ship
   or aircraft;
   (ii) against a ship, aircraft, persons or property in a place outside the jurisdiction of any State;
(b) any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft;
© any act inciting or of intentionally facilitating an act described in sub-paragraph (a) or (b)."

It may be reasonable to assume that piracy has existed Many pirates had roles in Chinese history since the Three Kingdoms period. An example includes Gan Ning of Eastern Wu.As early as 258 AD, the Gothic-Herulic fleet ravaged towns on the coasts of the Black Sea and Sea of Marmara. The Aegean coast suffered similar attacks a few years later. In 264, the Goths reached Galatia and Cappadocia, and Gothic pirates landed on Cyprus and Crete. In the process, the Goths seized enormous booty and took thousands into captivity.

In 286 AD, Carausius, a Roman military commander of Gaulish origins, was appointed to command the *Classis Britannica*, and given the responsibility of eliminating Frankish and Saxon pirates who had been raiding the coasts of Armorica and Belgic Gaul. In the Roman province of Britannia, Saint Patrick was captured and enslaved by Irish pirates.

Early Polynesian warriors attacked seaside and riverside villages. They used the sea for their hit-and-run tactics – a safe place to retreat to if the battle turned against them.

Among the unlawful acts covered by the SUA Convention in Article 3 are the seizure of ships by force; acts of violence against persons on board ships; and the placing of devices on board a ship which are likely to destroy or damage it.

The transportation of nuclear material is not considered an offence if such item or material is transported to or from the territory of, or is otherwise transported under the control of, a State Party to the Treaty on the Non Proliferation of Nuclear Weapons (Subject to conditions).

Under the new instrument, a person commits an offence within the meaning of the Convention if that person unlawfully and intentionally transports another person on board a ship knowing that the person has committed an act that constitutes an offence under the SUA Convention or an offence set forth in any treaty listed in the Annex. The Annex lists nine such treaties.

The new instrument also makes it an offence to unlawfully and intentionally injure or kill any person in connection with the commission of any of the offences in the Convention; to attempt to commit an offence; to participate as an accomplice; to organize or direct others to commit an offence; or to contribute to the commissioning of an offence.

A new Article requires Parties to take necessary measures to enable a legal entity (this could be a company or organization, for example) to be made liable and to face sanctions when a person responsible for management of control of that legal entity has, that capacity, committed an offence under the Convention

IMO Initiative

IMO is implementing an anti-piracy project, a long-term project which began in 1998. Phase one consisted of a number of regional seminars and workshops attended by Government representatives from countries in piracy-infested areas of the world; while phase two consisted of a number of evaluation and assessment missions to different regions. IMO's aim has been to foster the development of regional agreements on implementation of counter piracy measures.

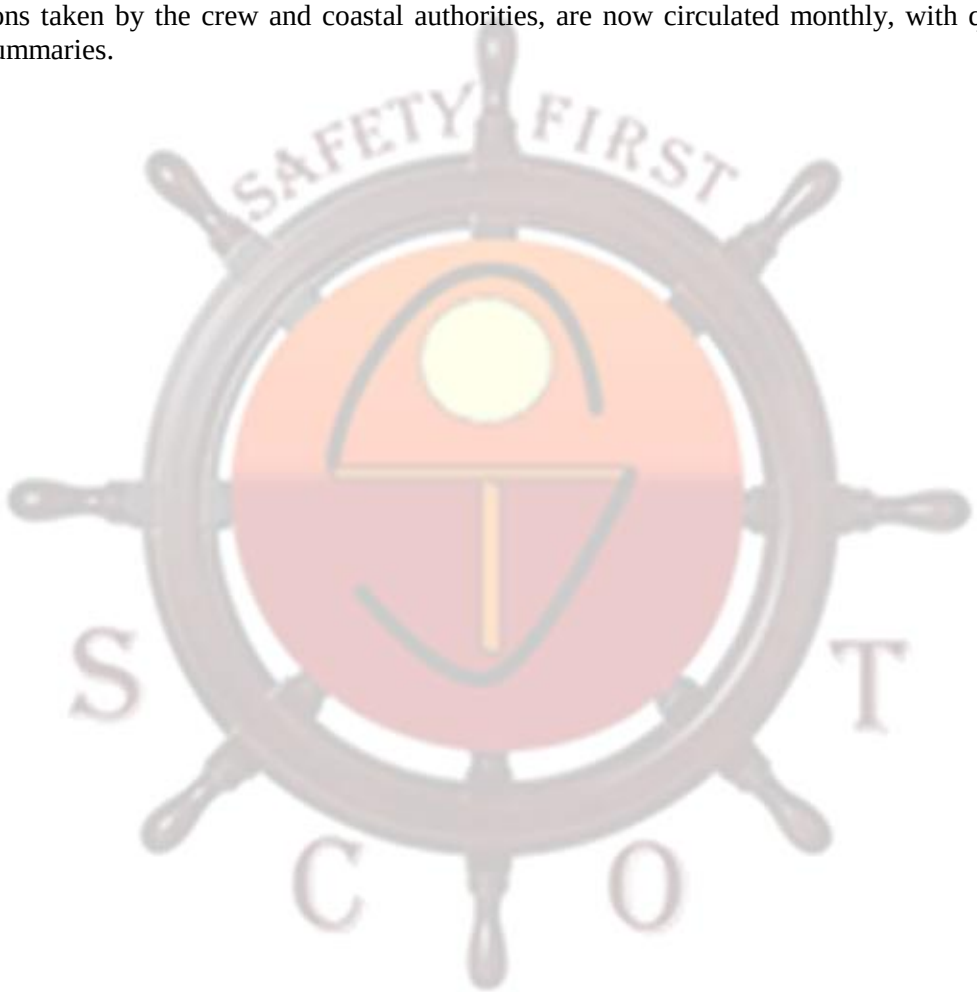
Regional cooperation among States has an important role to play in solving the problem of piracy and armed robbery against ships, as evidenced by the success of the regional anti-piracy operation in the Straits of Malacca and Singapore. The Regional Cooperation Agreement on Combating Piracy and Armed Robbery against ships in Asia (RECAAP), which was concluded in November 2004 by 16 countries in Asia, and includes the RECAAP Information Sharing Centre (ISC) for facilitating the sharing of piracy-related information, is a good example of successful regional cooperation which IMO seeks to replicate elsewhere.

Today, the deteriorating security situation in the seas off war-torn Somalia and the Gulf of Aden (and in the increasingly volatile Gulf of Guinea) are at the heart of the problem.

In January 2009, an important regional agreement was adopted in Djibouti by States in the region, at a high-level meeting convened by IMO. The Djibouti Code of Conduct concerning the Repression of Piracy and Armed Robbery against Ships in the Western Indian Ocean and the Gulf of Aden recognizes the extent of the problem of piracy and armed robbery against ships in the region and, in it, the signatories declare their intention to co operate to the fullest possible extent, and in a manner consistent with international law, in the repression of piracy and armed robbery against ships.

The signatories commit themselves towards sharing and reporting relevant information through a system of national focal points and information centres; interdicting ships suspected of engaging in acts of piracy or armed robbery against ships; ensuring that persons committing or attempting to commit acts of piracy or armed robbery against ships are apprehended and prosecuted; and facilitating proper care, treatment, and repatriation for seafarers, fishermen, other shipboard personnel and passengers subject to acts of piracy or armed robbery against ships, particularly those who have been subjected to violence.

To assist in anti-piracy measures, IMO issues reports on piracy and armed robbery against ships submitted by Member Governments and international organizations. The reports, which include names and descriptions of ships attacked, position and time of attack, consequences to the crew, ship or cargo and actions taken by the crew and coastal authorities, are now circulated monthly, with quarterly and annual summaries.



Chapter 12

Piracy off the Coast of Somalia

Piracy off the coast of Somalia is a major threat international shipping/trade since the second phase of the Somali Civil War in the early 21st century. The absence of an effective national coast guard following the outbreak of the civil war and the subsequent disintegration of the Armed Forces, local fishermen formed organized groups in order to protect their waters. This motivation is reflected in the names taken on by some of the pirate networks, such as the *National Volunteer Coast Guard*. However, as piracy has become substantially more lucrative in recent years, other reports have speculated that financial gain is now the primary motive for the pirates.

Since 2005, many international organizations, including the International Maritime Organization and the World Food Programme, have expressed concern over the rise in acts of piracy. Piracy has impeded the delivery of shipments and increased shipping expenses, costing an estimated $6.6 to $6.9 billion a year in global trade per Oceans Beyond Piracy (OBP).Combined Task Force 150, a multinational coalition task force, took on the role of fighting piracy off of the coast of Somalia by establishing a Maritime Security Patrol Area (MSPA) within the Gulf of Aden.

The Indian & International Efforts

The increasing threat posed by piracy has also caused concern in India since most of its shipping trade routes pass through the Gulf of Aden. The Indian Navy responded to these concerns by deploying a warship in the region on 23 October 2008. In September 2008, Russia announced that it too would join international efforts to combat piracy. Some reports have also accused certain government officials in Somalia of complicity with the pirates, with authorities from the Galmudug administration in the north-central Hobyo district reportedly attempting to use pirate gangs as a bulwark against Islamist insurgents from the nation's southern conflict zones.[19] However, according to UN Secretary-General Ban Ki Moon, both the former and current administrations of the autonomous Puntland region in northeastern Somalia appear to be more actively involved in combating piracy.

The latter measures include on-land raids on pirate hideouts, and the construction of a new naval base in conjunction with Saracen International, a UK-based security company. By the first half of 2010, these increased policing efforts by Somali government authorities on land and international naval vessels at sea reportedly contributed to a drop in pirate attacks in the Gulf of Aden from 86 a year prior to 33, forcing pirates to shift attention to other areas such as the Somali Basin and the wider Indian Ocean.

By the end of 2011, pirates managed to seize only four ships off of the coast of Somalia; 18 fewer than the 26 they had captured in each of the two previous years. They also attempted unsuccessful attacks on 52 other vessels, 16 fewer than the year prior. As of 11 March 2013, the pirates were holding 2 large ships with an estimated 60 hostages. It is estimated that, there were 151 attacks on ships in 2011, compared to 127 in 2010 - but only 25 successful hijacks compared to 47 in 2010. 10 vessels and 159 hostages were being held at February 2012. In 2011, pirates earned $146m, an average of $4.87m per ship.

Summary of recent events

Somali pirates have attacked hundreds of vessels in the Arabian Sea and Indian Ocean region, though most attacks do not result in a successful hijacking. In 2008, there were 111 attacks which included 42

successful hijackings.[42] However, this is only a fraction of the up to 30,000 merchant vessels which pass through that area.[43] The rate of attacks in January and February 2009 was about 10 times higher than during the same period in 2008 and "there have been almost daily attacks in March",[42] with 79 attacks,[44] 21 successful, by mid April. Most of these attacks occur in the Gulf of Aden but the Somali pirates have been increasing their range and have started attacking ships as far south as off the coast of Kenya in the Indian Ocean. Below are some notable pirate events which have garnered significant media coverage since 2007.On 28 January 2011, an Indian Coast Guard aircraft while responding to a distress call from the CMA CGM *Verdi*, located two skiffs attempting a piracy attack near Lakshadweep. Seeing the aircraft, the skiffs immediately aborted their piracy attempt and dashed towards the mother vessel, MV *Prantalay 14* – a hijacked Thai trawler, which hurriedly hoisted the two skiffs on board and moved westward. The Indian Navy deployed the INS *Cankarso* which located and engaged the mothership 100 nautical miles north of the Minicoy island. 10 pirates were killed while 15 were apprehended and 20 Thai and Burmese fishermen being held aboard the ship as hostages were rescued.

Within a week of its previous success, the Indian Navy captured another hijacked Thai trawler, MV *Prantalay 11* and captured 28 pirates aboard in an operation undertaken by the INS *Tir* purusuant to receiving information that a Greek merchant ship had been attacked by pirates on board high-speed boats, although it had managed to avoid capture. When INS *Tir* ordered the pirate ship to stop and be boarded for inspection, it was fired upon. The INS *Tir* returned fire in which 3 pirates were injured and caused the pirates to raise a white flag indicating their surrender. The INS *Tir* subsequently joined by CGS *Samar* of the Indian Coast Guard. Officials from the Indian Navy reported that a total of 52 men were apprehended, but that 24 are suspected to be Thai fishermen who were hostages of the 28 African pirates.In late February 2011, piracy targeting smaller yachts and collecting ransom made headlines when four Americans were killed aboard their vessel, the Quest, by their captors, while a military ship shadowed them. A federal court in Norfolk, Virginia, sentenced three members of the gang that seized the yacht to life imprisonment.[82] On 24 February 2011 a Danish family on a yacht were captured by pirates.

On Jan. 5 2012, an SH-60S Seahawk from the guided-missile destroyer USS Kidd, part of the USS John C. Stennis Carrier Strike Group, detected a suspected pirate skiff alongside the Iranian-flagged fishing boat, Al Molai. The master of the Al Molai sent a distress call about the same time reporting pirates were holding him captive.A visit, board, search and seizure team from the Kidd boarded the dhow, a traditional Arabian sailing vessel, and detained 15 suspected pirates who had been holding a 13-member Iranian crew hostage for several weeks. The Al Molai had been pirated and used as a "mother ship" for pirate operations throughout the Persian Gulf, members of the Iranian vessel's crew reported.

The methods used in a typical pirate attack have been analyzed. They show that while attacks can be expected at any time, most occur during the day, often in the early hours. They may involve two or more skiffs that can reach speeds of up to 25 knots. With the help of mother ships that include captured fishing and merchant vessels the operating range of the skiffs has been increased far into the Indian Ocean. An attacked vessel is approached from quarter or stern; RPGs and small arms are used to intimidate the operator to slow down and allow boarding. Light ladders are brought along to climb aboard. Pirates then will try and get control of the bridge to take operational control of the vessel. According to Sky News, pirates also often jettison their equipment in the sea before being arrested, as this lowers the likelihood of a successful prosecution.

Chapter 13

Anti-piracy measures

The third volume of the handbook: *Best Management Practices to Deter Piracy off the Coast of Somalia and in the Arabian Sea Area* (known as BMP3) is the current authoritative guide for merchant ships on self-defense against pirates. The guide is issued and updated by a consortium of interested international shipping and trading organizations including the EU, NATO and the International Maritime Bureau. It is distributed primarily by the Maritime Security Centre – Horn of Africa (MSCHOA) – the planning and coordination authority for EU naval forces (EUNAVFOR). BMP3 encourages vessels to register their voyages through the region with MSCHOA as this registration is a key component of the operation of the International Recommended Transit Corridor (IRTC) (the navy patrolled route through the Gulf of Aden). BMP3 also contains a chapter entitled "Self-Protective Measures" which lays out a list of steps a merchant vessel can take on its own to make itself less of a target to pirates and make it better able to repel an attack if one occurs. This list includes doing thing like ringing the deck of the ship with razor wire, rigging fire-hoses to spray sea-water over the side of the ship (to hinder boardings), having a distinctive pirate alarm, hardening the bridge against gunfire and creating a "citadel" where the crew can retreat in the event pirates get on board. Other unofficial self-defense measures that can be found on merchant vessels include the setting up of mannequins posing as armed guards or firing flares at the pirates.

Though it varies by country, generally peacetime law in the 20th and 21st centuries has not allowed merchant vessels to carry weapons. As a response to the rise in modern piracy, however, the U.S. Government changed its rules so that it is now possible for US-flagged vessels to embark a team of armed private security guards. Other countries and organisations have similarly followed suit. This has given birth to a new breed of private security companies who provide training and protection for crew members and cargo and have proved effective in countering pirate attacks. The USCG leaves it to ship owners' discretion to determine if those guards will be armed Seychelles has become a central location for international anti-piracy operations, hosting the Anti-Piracy Operation Center for the Indian Ocean. In 2008, VSOS became the first authorized armed maritime security company to operate in the Indian Ocean region.

With safety trials complete in the late 2000s, laser dazzlers have been developed for defensive purposes on super-yachts. They can be effective up to 2.5 miles with the effects going from mild disorientation to flash blindness at closer range. In February 2012, Italian Marines based on the tanker *Enrica Lexie* allegedly fired on an Indian fishing trawler off Kerala, killing two of her eleven crew. The Marines allegedly mistook the fishing vessel as a pirate vessel. The incident sparked a diplomatic row between India and Italy. *Enrica Lexie* was ordered into Kochi where her crew were questioned by officers of the Indian Police.[143] The fact is still *sub juris* and its legal eventual outcome could influence future deployment of VPDs, since states will be either encouraged or discouraged to provide them depending on whether functional immunity is ultimately granted or denied to the Italians.

Another similar incident has been reported to have happened in the Red Sea between the coasts of Somalia and Yemen, involving the death of a Yemeni fisherman allegedly at the hands of a Russian Vessel Protection Detachment (VPD) on board of a Norwegian flagged vessel. However, despite VPD deployment being controversial because of these incidents, according to the Associated Press,[147] during a United Nations Security Council conference about piracy "U.S. Ambassador Susan Rice told the council that no ship carrying armed guards has been successfully attacked by pirates" and "French Ambassador

Gerard Araud stressed that private guards do not have the deterrent effect that government-posted marine and sailors and naval patrols have in warding off attacks".

SUGGESTED PLANNING AND OPERATIONAL PRACTICES FOR OWNERS, OPERATORS, MANAGERS AND MASTERS OF SHIPS TRANSITING THE GULF OF ADEN AND OFF THE COAST OF SOMALIA PURPOSE

1. The purpose of this document is to provide Best Management Practices (BMP) to assist companies and ships in avoiding piracy attacks, deterring attacks and delaying successful attacks in the Gulf of Aden (GoA) and off the Coast of Somalia. The organizations consulted on this document represent the vast majority of ship owners and operators transiting the region.

2. These organizations will encourage their members to utilize these BMP and will endeavour to promulgate these to other shipping interests as BMP for combating piracy in the region. This document complements guidance provided in the IMO circular MSC.1/Circ.1334.

TYPICAL ATTACK PROFILES AND LESSONS LEARNT

1. During 2008, and the first half of 2009, an increase in the number of pirate attacks on merchant ships occurred throughout the GoA and off the coast of Somalia and within the wider North West Indian Ocean. The majority of attacks were initially clustered around the northern side of the GoA but attacks have occurred further off the east coast of Somalia.

2. Analysis of successful attacks indicates that the following common vulnerabilities are exploited by the pirates:

a. Low speed
b. Low freeboard
c. Inadequate planning and procedures
d. Visibly low state of alert and/or lack of evident self-protective measures
e. Where a slow response by the ship is evident

3. Commonly two or more small high-speed (up to 25 knots) open boats/"skiffs" are used in attacks often approaching from the port quarter and/or stern.

4. The use of a pirate "mother ship", which is a larger ship carrying personnel, equipment, supplies and smaller attack craft, has enabled attacks to be successfully undertaken at a greater range from the shore.

5. Vigilance should be highest at first light and last light, as the majority of the attacks have taken place during these periods.

6. Higher speed vessels (15 knots and above) should not presume to be safe from attack but speed is an effective form of defence. The use of small arms fire, Rocket Propelled Grenades (RPG), in an effort to intimidate masters of vessels to reduce speed has occurred within the area. Maintaining full sea speed in such circumstances has been shown to be effective.

7. The majority of attempted hijacks have been repelled by ship's crew who have planned and trained in advance of the passage and employed passive counter measures to good effect.

8. Prevailing weather and sea state conditions also greatly influence attackers' ability to operate. Wind strengths in excess of 18 knots and wave heights above 2 metres are considered sufficient to provide protection for all but the most vulnerable vessels, particularly where masters are taking full account of Best Management Practices.

RECOMMENDED BEST MANAGEMENT PRACTICES

1. Introduction

a. Whilst recognizing the absolute discretion of the master at all times to adopt appropriate measures to avoid, deter or delay piracy attacks in this region, this document of best practices is provided for shipowners and ship operators, masters and their crews.

b. Not all measures discussed in this document may be applicable for each ship. Therefore, as part of the risk analysis, an assessment is recommended to determine which of the BMP will be most suitable for the ship. The following have, however, generally proved effective:

2. Prior to Transit – General Planning

a. General

i. UKMTO Dubai is the first point of contact for ships in the region. The day-to-day interface between masters and the military is provided by UKMTO Dubai, who talk to the ships and liaise directly with MSCHOA and the naval commanders at sea. UKMTO Dubai require regular updates on the position and intended movements of ships. They use this information to help
the naval units maintain an accurate picture of shipping. (See Glossary at Annex A for further details.)

ii. The Maritime Security Centre – Horn of Africa (MSCHOA), is the planning and coordination authority for EU forces (EU NAVFOR) in the Gulf of Aden and the area off the Coast of Somalia. (See Glossary at Annex A.)

iii. The Marine Liaison Office (MARLO) operates as a conduit for information exchange between the Combined Maritime Forces (CMF) and the commercialshipping community within the region. (See Glossary at Annex A.)

iv. Prior to transiting the high risk area, the owner and master should carry out their own risk assessment to assess the likelihood and consequences of piracy attacks on the ship, based on the latest available information. The outcome of this risk assessment should identify measures for prevention, mitigation and recovery and will mean combining statutory requirements with supplementary measures to combat piracy.

v. Company crisis management procedures should consider appropriate measures to meet the threat of piracy by adopting IMO and other industry recommended practices as appropriate to the particular circumstances and ship type.

vi. Advanced notice of a vessel's intended passage is required by the naval authorities so that they can identify vulnerabilities and plan suitable protection. This is achieved by primarily:

1) Initial report to UKMTO Dubai, (e-mail or fax).
2) Initial report to MARLO (e-mail or fax).
3) Additionally, if planning to transit the Gulf of Aden, or navigate within the area bound by 12º N, 58º E & 10º S: Register the Vessel Movement with MSCHOA (either, online or by e-mail or fax).

vii. Whilst measures should be taken to prevent pirates boarding, the safety of crew and passengers is paramount.

b. Company Planning:

It is strongly recommended that managers and/or the operations department register for access to the restricted sections of the MSCHOA website (www.mschoa.eu), review the information contained therein and share this as appropriate within their fleet.

i. 4-5 days before the vessel enters the International Recommended Transit Corridor (IRTC), or area bound by 12 degrees North or 58 degrees East or 10 degrees South, ensure that a "Vessel Movement Registration" submission has been logged with MSCHOA (online, e-mail or fax) . Note: This can be done by either the ship or the company.

ii. Review the Ship Security Assessment (SSA) and implementation of the Ship Security Plan (SSP) as required by the International Ship and Port Facility Code (ISPS) to counter the piracy threat.

iii. The Company Security Officer (CSO) is encouraged to see that a contingency plan for the high risk passage is in place, exercised, briefed and discussed with the master and the Ship Security Officer (SSO).

iv. Be aware of the particular high risk sea areas that have been promulgated.

v. Offer their ship's master guidance with regard to the preferred and available methods of transiting the region (Group Transit, Escorted Group Transit, National Convoy, etc.).

vi. Conduct periodic crew training sessions.

vii. The use of additional private security guards is at the discretion of the company but the use of armed guards is not recommended.

viii. Consider additional resources to enhance watchkeeping numbers.

ix. Consider the outfitting of ships with Self Protection Measures (SPM) prior to transiting high-risk areas.

c. Ship's Master Planning:

i. Communication of "Initial Report" to UKMTO Dubai and MARLO (e-mail or fax) when entering the reporting area between Suez, and 78 degrees East 10 degrees South, see Anti-Piracy Planning chart Q6099.

ii. 4-5 days before entering the IRTC, or the area within 12 degrees North, 58 degrees East or 10 degrees South, ensure that a "Vessel Movement Registration" submission has been logged with MSCHOA (online, e-mail or fax). Note: This can be done by either the ship or the company. If it is completed by the company, masters should satisfy themselves with their companies that their details are correctly registered with MSCHOA.

iii. Prior to transit of the region it is recommended that the crew should be thoroughly briefed.

iv. The anti-piracy contingency plan has been shown to be most effective when implemented in advance. A drill is conducted prior to arrival in the area, the plan reviewed and all personnel briefed on their duties, including familiarity with the alarm signal signifying a piracy attack.

v. Masters are advised to also prepare an emergency communication plan, to include all essential emergency contact numbers and pre-prepared messages, which should be ready at hand or permanently displayed near the communications panel (e.g., telephone numbers of MSCHOA,IMB PRC,CSO, etc. – see Contact List at Annex B).

vi. Define the ship's AIS policy: SOLAS permits the master the discretion to switch off AIS if he believes that its use increases the ship's vulnerability. However, in order to provide naval forces with tracking information within the GoA it is recommended that AIS transmission is continued but restricted to ship's identity, position, course, speed, navigational status and safety-related information. Off the coast of Somalia the decision is again left to the master's discretion, but current Naval advice is to turn it off completely. If in doubt this can be verified with MSCHOA.

3. Prior to Transit Voyage Planning

a. Vessels are encouraged to report their noon position, course, speed, estimated and actual arrival times to UKMTO Dubai and MARLO whilst operating in the region. b. Vessels are also encouraged to increase the frequency of such reports when navigating in known high risk/piracy areas and further report upon passing Point A or B in the GoA, as shown on Anti-Piracy Chart Q6099.

c. Inside the GoA

i. EUNAVFOR strongly recommends that ships conduct their passage within the IRTC. Westbound ships should bias themselves to the northern portion of the corridor, and eastbound ships to the southern portion. Group Transit (GT) guidance within the GoA for times and speeds are on the MSCHOA website, if a GT is contemplated.

ii. Ships should avoid entering Yemeni Territorial Waters (YTWs) while on transit. This is for reasons of customary international law, as it is not possible for international military forces (non-Yemeni) to protect ships that are attacked inside Yemeni TTW.

iii. Ships may be asked to make adjustments to passage plans to conform to MSCHOA routeing advice.

iv. During GTs ships should not expect to be permanently in the company of a warship. But all warships in the GoA, whether part of EUNAVFOR or coordinating with them, will be aware of the GoA GTs and will have access to the full details of vulnerable shipping.

v. MSCHOA strongly recommends masters make every effort to plan transit periods of highest risk areas of the GoA for night passage (MSCHOA will advise ships). Very few successful attacks have occurred at night.

d. Outside the GoA

i. Ships navigating off the east coast of Somalia should consult with the MSCHOA website or UKMTO Dubai in order to obtain the most recent routeing advice.
ii. Masters should still update UKMTO Dubai in the usual manner with their ship's course and details.
e. A list of useful contact details are contained in Annex B.

4. Prior to Transit – Defensive Measures

a. Taking into account the manning levels, ensure that ship routines are adjusted sufficiently in advance so that well-rested and well-briefed crew are on watch and sufficient watch keepers are available. The Master and Officers of the Watch should be familiar with the impact of zig-zag manoeuvres on board their particular ship, (in all sea conditions) and in particular the impact that these manoeuvres can have upon reducing the speed of the vessel.

b. Consider minimizing external communications (radios, handsets and AIS information) to essential safety- and security-related communication and SOLAS information only, during transit of the GoA and passing the Coast of Somalia.

c. Increase readiness and redundancy by running additional auxiliary machinery, including generators and steering motors.

d. Increase lookouts/bridge manning.

e. Man the engine-room.

f. Secure and control access to the bridge, engine-room, steering gear room, and all accommodation /internal spaces. All potential access points (doors, portholes, vents, etc.) should be risk-assessed and adequately secured, especially where the potential access point is considered large enough for an attacker to gain entry. Access to and from the accommodation and internal work spaces should be reduced to a single point of entry when transiting the high risk areas. Any measures employed should not obstruct an emergency EXIT from within the internal space, whilst remaining secure from access by pirates outside.

g. In case of emergency, warships can be contacted on VHF Ch. 16 (Backup Ch.08).

h. Check all ladders and outboard equipment are stowed or up on deck.

i. Check that self-protection measures put in place in advance remain securely fitted and function as intended. Be mindful that temporary devices may work loose and consequently may only provide a reduced level of protection.

j. If the ship has a comparatively low freeboard, consider the possibility of extending the width of the gunwales to prevent grappling hooks from gaining hold. Check the MSCHOA website for examples of such measures.

k. It is recommended that a piracy attack muster point or “citadel” be designated and lock-down procedures rehearsed in order to delay access to control of the ship and buy time. Ideally this should be away from external bulkheads and portholes. Due to the ongoing debate on the use of citadels and their method of employment, masters are recommended to check regularly with MSCHOA.

l. Consider the use of dummies at the rails to simulate additional lookouts. However, if ship design creates lookout black spots and the security assessment identifies this risk, then it may have to be covered by manpower.

m. It is suggested fire pumps and/or hoses should be pressurised and ready for discharge overboard around the vessel, particularly at the most vulnerable points.

n. Consideration should also be given to creating a water curtain around the vessel to further deter boarding.

o. Consider the use of razor wire/physical barriers around stern/lowest points of access, commensurate with crew safety and escape.

p. Consider the use of passive defence equipment.

q. Consider providing night vision optics for use during the hours of darkness.

5. In Transit – Operations

a. Ship's crew should not be exposed to undue risk when employing Self-Protective Measures (SPM).

b. All ships inside the GoA are strongly urged to use the IRTC and follow MSCHOA GT advice and timings as promulgated on the MSCHOA web site.

c. Attention of Mariners is also drawn to IMO circular SN.1/Circ.281 dated 4 August 2009, *"Information on Internationally Recognised Transit Corridor (IRTC) for Ships Transiting the Gulf of Aden"* where advice is provided that the IRTC is subject to change by military authorities according to prevailing circumstances. Mariners are therefore urged to obtain up-to-date information from the "MSCHOA" website http://www.mschoa.org or NAV-warnings promulgated for that area.

d. If you intend to follow a Group Transit (GT) through the IRTC: Transit at the group transit speed, but remain aware of the ship's limitations. (Current advice, for example, is that if your full sea speed is 16 knots, consider joining a 14 knot GT and keep those 2 knots in reserve.)

e. If you do not intend to follow a GT through the IRTC: Maintain full sea speed through the high risk area. (Current advice is that if the full sea speed of the ship is more than 18 knots, then do not slow down for a GT. Instead, maintain full sea speed and aim to transit as much of the high risk area in darkness as possible.)

f. Ships should comply with the International Rules for Prevention of Collision at Sea at all times. Masters should endeavour not to impede the safe navigation of other vessels when joining and leaving the IRTC. Navigation lights should not be turned off at night. Follow the guidance given by Flag State Authority.

g. Provide deck lighting only as required for safety. Lighting in the shadow zones around the ship's hull may extend the area of visibility for lookouts, but only where consistent with safe navigation. Where fitted, and deemed suitable, consider the immediate use of "remotely operated" ship search lights, if suspicious activity around the vessel is observed, the use of search lights may startle and deter a potential attack. (Current Naval advice is to transit with navigation lights only).

h. Keep photographs of pirate "mother ships" on the bridge. Report immediately if sighted. Report all sightings of suspect mother ships to UKMTO Dubai and the IMB PRC. (See Annex C for an example of a Piracy Report for passing on such information or reporting on any other attack or sighting.)

i. The master should try to make as early an assessment of a threat as possible. As soon as the master feels that a threat is developing he should immediately call the UKMTO Dubai.

j. Keep a good lookout by all available means for suspicious craft, especially from astern and each quarter.

k. Protect the crew from exposure to undue risk. Only essential work on deck should occur in transit of the high risk area. Masters should, in so far as possible, keep crew members clear from external deck spaces during hours of darkness, whilst being mindful of their obligation to maintain a full and proper lookout at all times.

l. Use light, alarm bells and crew activity to alert suspected pirates that they have been detected.

m. A variety of other additional commercially available non-lethal defensive measures are available that could be considered; however these should be assessed by companies on their merits and on the particular characteristics and vulnerability of the ship concerned.

6. If Attacked by Pirates

a. Follow the ship's pre-prepared contingency plan.

b. Activate the Emergency Communication Plan, and report the attack immediately to the single primary point of contact in the event of an attack, which is UKMTO Dubai. *(MSCHOA, as the continually manned maritime security watch centre for piracy attacks in the region, will continue to function as a back-up contact point in the event of an attack).*

c. Activate the Ship Security Alert System (SSAS), which will alert your Company Security Officer and flag state. *Post attack reports should be communicated as quickly as possible to all relevant piracy reporting centres as explained in section 9.*

d. If the master has exercised his right to turn off the Automatic Identification System (AIS) during transit of the piracy area, this should be turned on once the ship comes under pirate attack.

e. Sound the emergency alarm and make a 'pirate attack' (PA) announcement in accordance with the ship's emergency plan.

f. Make a “Mayday” call on VHF Ch. 16 (and backup Ch. 08, which is monitored by naval units). Send a distress message via the DSC (Digital Selective Calling) system and Inmarsat-C, as applicable. Establish telephone communication with UKMTO Dubai.

g. Prevent skiffs closing on the ship by altering course and increasing speed where possible1. Pirates have great difficulty boarding a ship that is:
i. Making way at over 15 knots.
1: If you can buy time until the military forces arrive, this often leads the pirates to abort their attack. This is why early
registration with MSCHOA, use of Group Transit timings and updating your position with UKMTO Dubai are all
essential: it gives a better probability that Naval support will be nearby if the pirates attack.

ii. Manoeuvring – it is suggested that as early as possible masters undertake continuous small zigzag manoeuvres to further deter boarding whilst maintaining speed. Consider increasing the pirates' exposure to wind/waves and using bow wave and stern wash to restrict pirate craft coming alongside.

Masters and the Officer of the Watch (OOW) should be aware of the handling and manoeuvring characteristics of the vessel. Particular attention should be given to the effects of varying helm orders and the impact these can have on the ship's speed.

h. Activate fire pump defensive measures.

i. Consider turning on forward facing deck lights to draw attention to your vessel and aid positive identification by arriving military forces as a vessel under attack.

j. Muster all remaining crew in accordance with the ship's contingency plan.

7. If Boarded by Pirates

a. Before pirates gain access to the bridge, inform UKMTO Dubai and, if time permits, the Company.

b. Offer no resistance; this could lead to unnecessary violence and harm to the crew.

c. If the bridge/engine-room is to be evacuated, then the main engine should be stopped; all way taken off the vessel if possible and the ship navigated clear of other ships.

d. Remain calm and cooperate fully with the pirates.

e. Ensure all crew, other than the bridge team, stay together in one location.

f. If in a locked down "citadel" ensure internal protection/cover is available in case the pirates attempt to force entry. Keep clear of entry point/doors and portholes/windows – do not resist entry. Use citadel emergency communication methods to communicate with authorities.

8. In the Event of Military Action

a. Crew should be advised NOT to use cameras with flash at any time when any military action is underway.

b. In the event that military personnel take action on board the ship, all personnel should keep low to the deck, cover their head with both hands, with hands visible and empty.

c. Be prepared to answer questions on identity and status on board.

d. Be aware that English is not the working language of all naval units in the region.

e. Military Forces may initially secure all persons encountered. This is standard practice. Brief and prepare ship's personnel to expect this and to cooperate fully during the initial stages of military action on board.

9. Post Incident Reporting (Reference Annex C)

f. Following any piracy attack or suspicious activity, it is vital that a detailed report of the event is reported to MSCHOA, UKMTO DUBAI and the IMB.

g. This will ensure full analysis and trends in piracy activity are established as well as enabling assessment of piracy techniques or changes in tactics, in addition to ensuring appropriate warnings can be issued to other Merchant shipping in the vicinity.

h. Masters are therefore requested to complete the standardized piracy report form contained in Annex C.

Updating Best Management Practices

1. It is anticipated that these BMP will be periodically updated based upon operational experience and lessons learned. The parties to this document will endeavour to meet regularly to update these BMP and to circulate revisions to their respective members and other interested organizations.

2. If in doubt, consult the MSCHOA website where additional relevant information will always be posted (noting that this may not be endorsed by all of the above-listed organizations).

ANNEX A: GLOSSARY

The roles and interrelationship of the coordinating bodies involved.

EUNAVFOR

EUNAVFOR is the coordinating authority which operates the Maritime Security Centre (Horn of Africa). All information and contact details are to be found within the MSCHOA website.

MSC (HOA) Maritime Security Centre (Horn of Africa)

MSCHOA was set up by the European Union (EU) as part of a European Security and Defence Policy initiative to combat piracy in the Horn of Africa. This work commenced with the establishment of EU NAVCO in September 2008. This Coordination Cell working in Brussels established links with a broad cross-section of the maritime community and provided coordination with EU forces operating in the region. In November 2008, the Council of the European Union took a major step further by setting up a naval mission – EU NAVFOR ATALANTA – to improve maritime security off the Somali coast by preventing and deterring pirate attacks and by helping to safeguard merchant shipping in the region.

UKMTO Dubai – (UK) Maritime Trade Operations

The UK Maritime Trade Operations (UKMTO Dubai) office in Dubai acts as a point of contact for industry liaison with the Combined Military Forces (CMF). UKMTO Dubai also administers the Voluntary Reporting Scheme, under which merchant ships are encouraged to send daily reports, providing their position and ETA at their next port, whilst transiting the region bound by Suez, 78°E and 10°S. UKMTO Dubai subsequently tracks ships, and the positional information is passed to CMF and EU headquarters. Emerging and relevant information affecting commercial traffic can then be passed directly to ships, rather than by company offices, improving responsiveness to any incident and saving time.

ANNEX C: FOLLOW-UP REPORT – PIRACY ATTACK REPORT VESSEL PARTICULARS/DETAILS:

1 NAME OF SHIP:
2 IMO No.:
3 FLAG:
4 CALL SIGN
5 TYPE OF SHIP:
6 TONNAGES: GRT: NRT DWT:
7 OWNERS (ADDRESS & CONTACT DETAILS):

8 MANAGERS (ADDRESS & CONTACT DETAILS):
9 LAST PORT/NEXT PORT:
10 CARGO DETAILS:
(TYPE/QUANTITY)

DETAILS OF INCIDENT

11 DATE & TIME OF INCIDENT: LT UTC
12 POSITION: LAT: (N/S) LONG: (E/W)
13 NEAREST LAND MARK/LOCATION:
14 PORT/TOWN/ANCHORAGE AREA:
15 COUNTRY/NEAREST COUNTRY:
16 STATUS (BERTH/ANCHORED/STEAMING):
17 OWN SHIP'S SPEED :
18 SHIP'S FREEBOARD DURING ATTACK :
19 WEATHER DURING ATTACK (RAIN/FOG/MIST/CLEAR/ETC., WIND (SPEED AND DIRECTION), SEA/SWELL HEIGHT) :
20 TYPES OF ATTACK (BOARDED/ATTEMPTED):
21 CONSEQUENCES FOR CREW, SHIP AND CARGO:
ANY CREW INJURED/KILLED:
ITEMS/CASH STOLEN :
22 AREA OF THE SHIP BEING ATTACKED:
23 LAST OBSERVED MOVEMENTS OF PIRATES/SUSPECT CRAFT

DETAILS OF RAIDING PARTY

23 NUMBER OF PIRATES/ROBBERS:
24 DRESS/PHYSICAL APPEARANCE:
25 LANGUAGE SPOKEN:
26 WEAPONS USED:
27 DISTINCTIVE DETAILS:
28 CRAFT USED:
29 METHOD OF APPROACH:
30 DURATION OF ATTACK:
31 AGGRESSIVE/VIOLENT:

FURTHER DETAILS
32 ACTION TAKEN BY MASTER AND CREW:
33 WAS INCIDENT REPORTED TO THE COASTAL AUTHORITY? IF SO TO WHOM?
34 PREFERRED COMMUNICATIONS WITH REPORTING SHIP: APPROPRIATE COAST RADIO STATION/HF/MF/VHF/INMARSAT IDS (PLUS OCEAN REGION CODE)/MMSI
34 ACTION TAKEN BY THE AUTHORITIES:
35 NUMBER OF CREW/NATIONALITY:
36 PLEASE **ATTACH** WITH THIS REPORT – **A** BRIEF DESCRIPTION/FULL REPORT/ MASTER – CREW STATEMENT OF THE ATTACK/PHOTOGRAPHS TAKEN IF ANY
***